AMENDMENTS TO THE CLAIMS:

Please cancel claims 5-8, 24-28, 31, and 32 without prejudice or disclaimer:

1. (Previously Presented) A method of processing semiotic data, comprising:

receiving semiotic data including at least one data set P;

selecting a function h, and for at least one of each said data set P to be collected, computing h(P);

destroying said data set P;

storing h(P) in a database, and

obtaining a sample of P' such that a comparison can be made;

at least one of obtaining and computing h(P'); and

to determine whether P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether P' substantially matches, but does not exactly match, one of said data set P,

wherein said data set P cannot be extracted from h(P),

wherein said semiotic data comprises biometric data,

wherein said function h comprises a secure hash function,

wherein the data set P is not determined perfectly by its reading,

wherein each reading gives a number Pi, wherein i is no less than 0, wherein P0 is for an initial reading, and a secret version of said initial reading is stored after further processing thereof,

wherein reading P0 is different from Pi for $i > 0$, and the secret version of P0 is different from the secret version of Pi, such that no identification is possible by a direct comparison of the encrypted data,

said method further comprising:

extracting sub-collections Sj from the collection of data in data set P;

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability,

comparing encrypted versions of the sub-collections Sj with those data stored in said database,

wherein if one or more of the sub-collection Sj matches with said data, then verification is deemed to have occurred,

each time a Pi, with $i > 0$, is read, computing all possible predetermined size variations of Pi which correspond to an acceptable predetermined imprecision of the reading; and

encrypting all such modified data, and comparing said encrypted modified data to data stored in said database,

wherein for a plurality of users of the same biometric information, said biometric information is encrypted differently for each user, and

wherein at least one of said data set P and P' comprises a personal data set.

2-8. (Canceled)

9. (Previously Presented) A method of processing semiotic data, comprising:

receiving semiotic data including at least one data set P;

selecting a function h, and for at least one of each said data set P to be collected, computing h(P);

destroying said data set P;

storing h(P) in a database,

wherein said data set P cannot be extracted from h(P),

wherein the data set P is not determined perfectly by its reading,

wherein each reading gives a number Pi, wherein i is no less than 0, wherein P0 is for an initial reading, and a secret version of said initial reading is stored after further processing thereof,

wherein reading P0 is different from Pi for $i > 0$, and the secret version of P0 is different from the secret version of Pi, such that no identification is possible by a direct comparison of the encrypted data;

extracting sub-collections Sj from the collection of data in data set P; and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

10. (Canceled)

11. (Previously Presented) The method according to claim 9, further comprising:

comparing encrypted versions of the sub-collections Sj with those data stored in said database,

wherein if one or more of the sub-collection Sj matches with said data, then verification is deemed to have occurred.

12. (Original) The method according to claim 11, further comprising:

each time a Pi, with $i > 0$, is read, computing all possible predetermined size variations of Pi which correspond to an acceptable predetermined imprecision of the reading; and

encrypting all such modified data, and comparing said encrypted modified data to data stored in said database.

13. (Original) The method according to claim 12, wherein for a plurality of users of the same biometric information, said biometric information is encrypted differently for each user.

14. (Previously Presented) The method according to claim 1, wherein at least one of said data set P and P' comprises a personal data set.

15. (Previously Presented) A method of processing biometric data, comprising:

acquiring unencrypted biometric data including at least one data set P;

encrypting, with one of a secure hash function and an identity function, each said at least one data set acquired;

destroying the unencrypted data set P;

storing each of the at least one encrypted data set in a database,

wherein unencrypted biometric data is not available nor retrievable from said data stored in said database, and

to determine whether a data set P' is a predetermined subject, comparing an encrypted data set of P' to the at least one encrypted data set stored in the database to determine whether the data set P' substantially matches, but does not exactly match, the at least one encrypted data set stored in the database,

said method further comprising:

extracting sub-collections Sj from the collection of data in data set P;

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability,

comparing encrypted versions of the sub-collections Sj with those data stored in said database,

wherein if one or more of the sub-collection Sj matches with said data, then verification is deemed to have occurred.

16. (Previously Presented) The method according to claim 15, wherein at least one of said data set P and P' comprises a personal data set.

17. (Previously Presented) A method of extracting components of biometric data which are stable under measurement errors, comprising:

acquiring unencrypted biometric data including at least one data set P;

encrypting each said at least one data set acquired to form at least one encrypted data set;

destroying the unencrypted data set P;

storing each said at least one encrypted data set in a database,

wherein unencrypted biometric data is not available nor retrievable from said data stored in said database, and

to determine whether a data set P' is a predetermined subject, comparing an encrypted data set of P' to the at least one encrypted data set stored in the database to determine whether there is a match,

said method further comprising:

extracting sub-collections Sj from the collection of data in data set P;

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability,

comparing encrypted versions of the sub-collections Sj with those data stored in said database,

wherein if one or more of the sub-collection Sj matches with said data, then verification is deemed to have occurred.

18. (Previously Presented) The method according to claim 17, wherein at least one of said data set P and P' comprises a personal data set.

19. (Original) A method of extracting components of biometric data which are stable under measurement errors, comprising:

acquiring unencrypted biometric data including at least one data set P;

encrypting each said at least one data set acquired to form at least one encrypted data set;

destroying the unencrypted data set P; and

storing each said at least one encrypted data set in a database,

wherein unencrypted biometric data is not available nor retrievable from said data stored in said database,

extracting sub-collections Sj from the collection of data in said data set P; and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

20. (Original) The method according to claim 19, wherein said data set comprises a personal data set.

21. (Original) The method according to claim 19, further comprising:

comparing encrypted versions of the sub-collections Sj with those data stored in said database,

wherein if one or more of the sub-collection Sj matches with said data, then verification is deemed to have occurred.

22. (Original) The method according to claim 21, wherein a data set P is not determined perfectly by its reading, such that each reading gives a number Pi,

wherein i is no less than 0,

wherein P0 is for an initial reading, and a secret version of said initial reading is stored after further processing thereof,

wherein reading P0 is different from Pi for $i > 0$, and the secret version of P0 is different from the secret version of Pi, such that no identification is possible by a direct comparison of the encrypted data.

23. (Original) The method according to claim 21, further comprising:

each time a data set is read Pi, with $i > 0$, is read, computing all possible predetermined size variations of Pi which correspond to an acceptable predetermined imprecision of the reading; and

encrypting all such modified data, and comparing said encrypted modified data to data stored in said database.

24-28. (Canceled)

29. (Original) A system for extracting components of biometric data which are stable under measurement errors, comprising:

acquiring unencrypted biometric data including at least one data set P; encrypting each said at least one data set acquired to form at least one encrypted data set;

destroying the unencrypted data set P; and

storing each said at least one encrypted data set in a database,

wherein unencrypted biometric data is not available nor retrievable from said data stored in said database,

extracting sub-collections Sj from the collection of data in said data set P; and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

30. (Previously Presented) The system according to claim 29, wherein said data set comprises a personal data set.

31. (Canceled)

32. (Canceled)

33. (Previously Presented) A computer-readable medium tangibly embodying a program of machine-readable instructions executable by a digital processing apparatus to perform a

method for computer-implemented verifying of biometric data without storing unencrypted biometric data, said method comprising:

acquiring unencrypted biometric data including at least one data set P;

encrypting each said at least one data set acquired to form at least one encrypted data set;

destroying the unencrypted data set P;

storing each said at least one encrypted data set in a database, wherein unencrypted biometric data is not available nor retrievable from said data stored in said database, and

to determine whether a data set P' is close to a predetermined subject, comparing an encrypted data set of P' to said at least one encrypted data set to determine whether data set P' is close to some data set P,

said method further comprising:

extracting sub-collections Sj from the collection of data in data set P;

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability,

comparing encrypted versions of the sub-collections Sj with those data stored in said database,

wherein if one or more of the sub-collection Sj matches with said data, then verification is deemed to have occurred.

34. (Previously Presented) The computer-readable medium according to claim 33, wherein at least one of said data set P and P' comprises a personal data set.

35. (Previously Presented) A computer-readable medium tangibly embodying a program of recordable, machine-readable instructions executable by a digital processing apparatus to perform a method for computer-implemented extracting components of biometric data which are stable under measurement errors, said method comprising:

acquiring unencrypted biometric data including at least one data set P; encrypting each said at least one data set acquired to form at least one encrypted data set;

destroying the unencrypted data set P;

storing each said at least one encrypted data set in a database, wherein unencrypted biometric data is not available nor retrievable from said data stored in said database;

extracting sub-collections Sj from the collection of data in said data set P; and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

36. (Previously Presented) The computer-readable medium according to claim 35, wherein said data set comprises a personal data set.